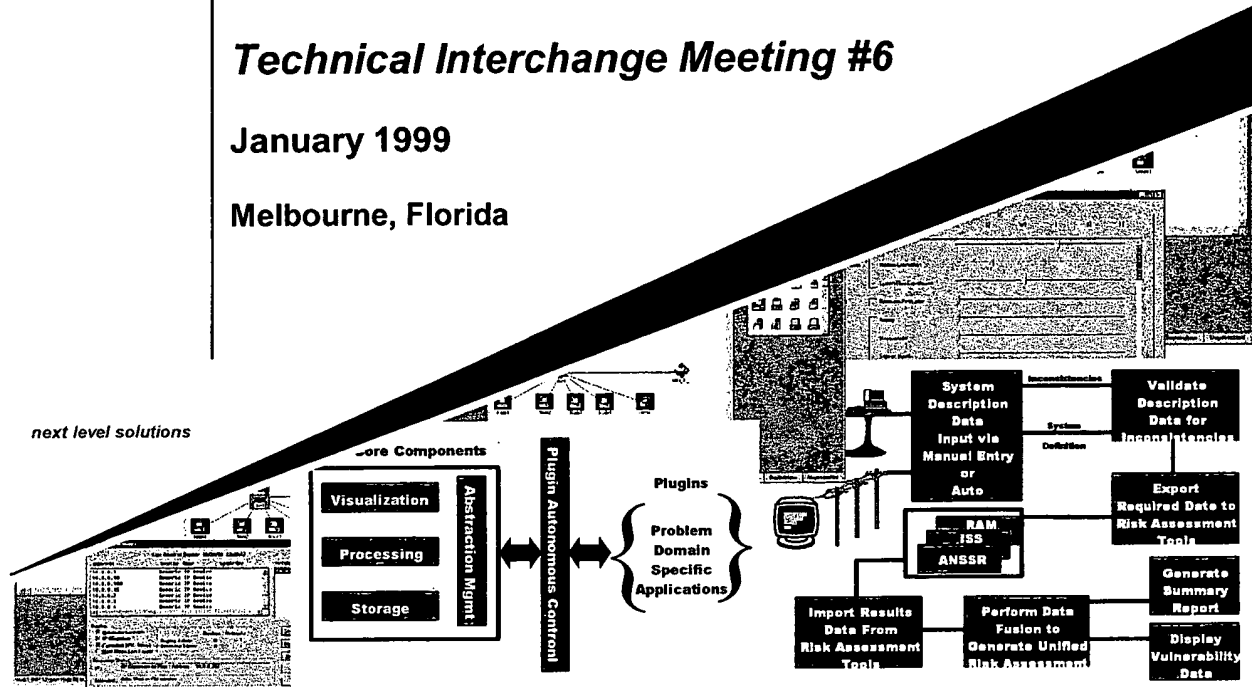


Network Visualization Tool (NVT) Program

Technical Interchange Meeting #6

January 1999

Melbourne, Florida



Introductions

Click to add sub-title

Agenda - Day 1



Time	Topic
0815	Check-in
0830	Welcome & Introduction
0900	NVT Program Goals and Objectives
0930	Roundtable 1 – Do the goals of NVT map to the community needs and requirements?
1015	Break
1030	Information Sharing – RAM and DPL-f
1100	NVT Design – Overall Architecture
1200	Working Lunch
1300	NVT Demonstration – (1) Automatic Discovery (1) Manual Network Diagram
1400	NVT Design – Object Classes
1445	Break
1500	COTS Integration Lessons Learned
1530	Plans for Next Quarter
1600	Roundtable 2 – Feedback on Proof-of-Concept Prototype
1630	Wrap Up

Agenda - Day 2



Time	Topic
0815	Check-in
0830	Overview
0845	Protocol Mining / LANmine
1015	Break
1030	STAKEOUT
1200	Working Lunch
1230	STAT
1430	Briefing Center Tour

NVT Program Overview and Objectives

Click to add sub-title

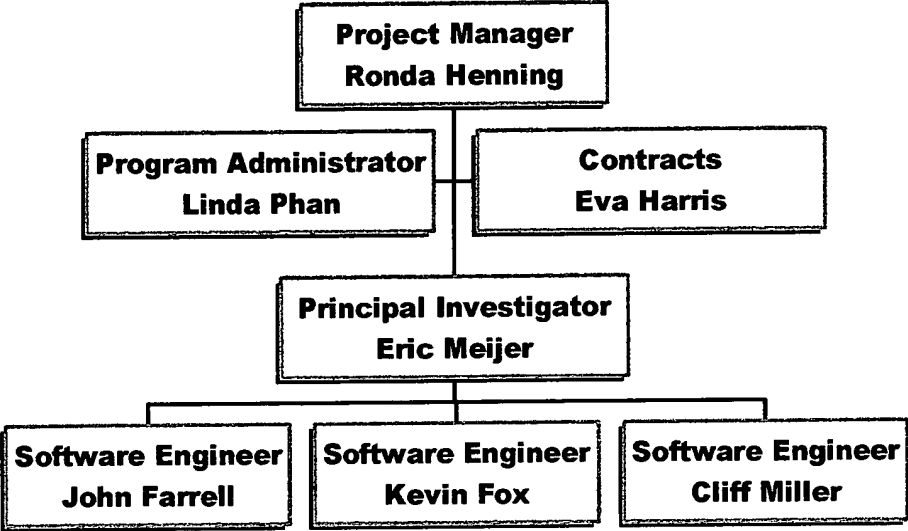
Program Overview



- **Customer: AFRL/IFGB**
 - *LPM: Dwayne Allain*
 - *Deputy: Peter Radesi*
- **Value: \$573K**
- **Schedule: 24 months, 1 April 1997 start**
- **Objectives**
 - *Investigate current risk assessment and vulnerability detection products to determine if they can be incorporated into a common framework*
 - *Investigate technologies for the enhancement of automated risk assessment technology in the areas of usability, productivity and capability*

- **Objectives (continued)**

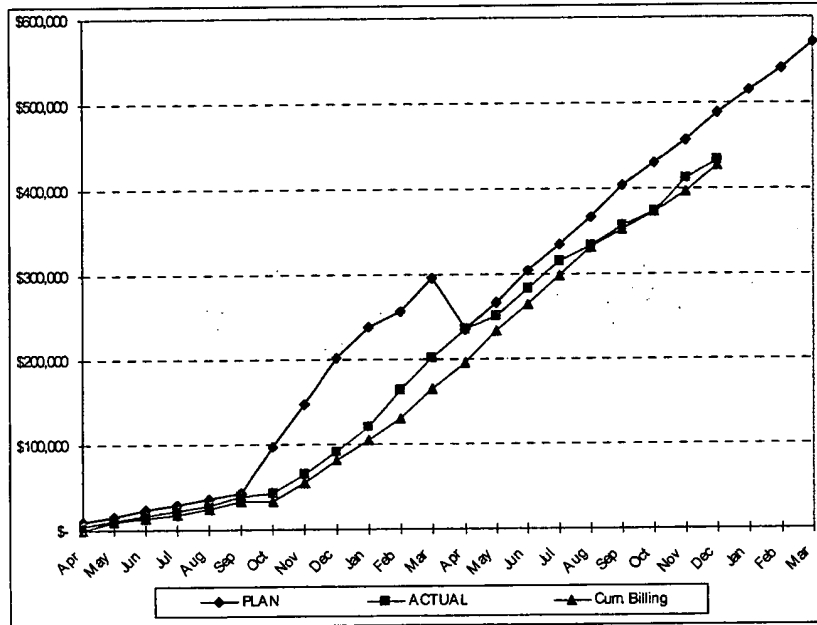
- *In particular, investigate enhancement through*
 - Methods to perform knowledge solicitation
 - Normalized system representation satisfying the needs of several existing risk assessment tools
 - Fusion of various tool outputs into a single report
 - Graphical display of the resulting vulnerability data
- *Develop an initial Proof-of-Concept prototype*



Financial Summary



- Expenditures



Through December
Planned: \$488.7K
Actuals: \$433.5K

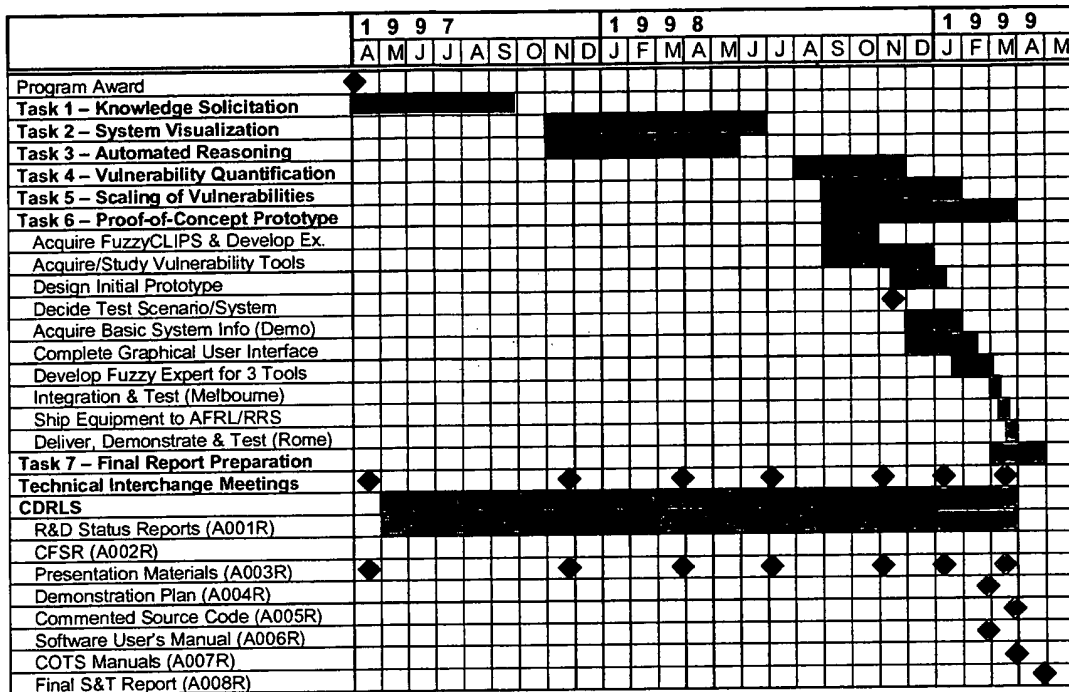
Program Schedule



- **Contract began 1 April 1997**
- **24 month schedule, divided into 7 tasks**
 - *Task #1 - Knowledge Solicitation*
 - *Task #2 - System Visualization and Validation*
 - *Task #3 - Selection and Application of Automated Reasoning Technologies (Risk Assessment Tools)*
 - *Task #4 - Vulnerability Quantification*
 - *Task #5 - Scaling of Identified Vulnerabilities*
 - *Task #6 - Proof-of-Concept Prototype*
 - *Task #7 - Final Report*

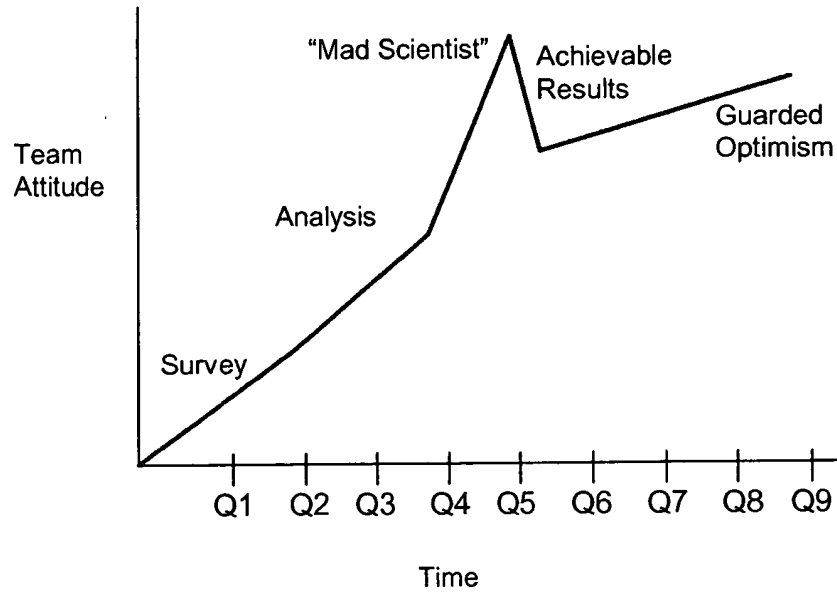
- **Task #1 - Knowledge Solicitation - Completed**
 - *Resulted in selection of OpenView as discovery technology*
 - *Also have NET VIZ in NVT Lab*
- **Task #2 - System Visualization & Validation - On-going**
- **Task #3 - Selection & Application of Automated Reasoning Technologies - Completed**
 - *Resulted in selection of ANSSR, ISS, and RAM*
- **Task #4 - Vulnerability Quantification**
- **Task #5 - Scaling of Identified Vulnerabilities - Underway**
 - *Resulted in selection of Fuzzy Expert System technology to integrate results from risk assessment tools*
- **Task #6 - Proof-of-Concept Prototype - Underway**
 - *Demonstration of initial Proof-of-Concept Prototype today*
- **Task #7 - Final Report**

Milestone Schedule



- Feasible to use multiple tools to fill in missing data.
- Tools with different modes of operation can be combined to provide a more complete picture.
- It is possible to combine the results of multiple tools into one coherent picture.
- Fusion techniques are viable for use in report integration.

Phases of NVT



What is Risk?

- **Risk includes: assessment, characterization, communication, management, and policy relating to risk**
- **How do we quantify risk?**
- **How do organizations respond to *vague* risks?**
 - *Who specifies the situational factors?*
- **At what point does an organization respond to a risk?**
 - *How are different strategies identified and then deployed?*
- **How is a risk response(response strategy) defined?**

NVT Architecture Goals

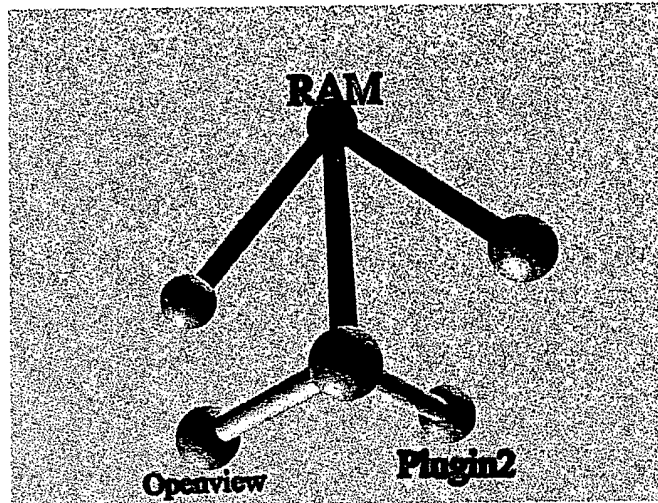


- Establish a framework that allows for the use of current, and future, vulnerability and risk assessment *Plugins* (the collective set of third party applications a user wishes to integrate into the NVT system)
- The Framework shall establish the foundation for a system that can resolve Knowledge & Language issues
- Provide the user with a clear understanding of their present risk based on the most effective use of the current *Plugin* set
- Provide the user with the capability to determine the most effective means to mitigate their risk

NVT must provide *rational* probable solutions

Plugin Relationships

HARRIS
Electronic Systems



Today



- **"Grounded" in feasible, incremental improvement**
- **Near term results that will have a positive impact**
- **Useful demonstration system**
- **Tangible end products**

Your Chance to . . .



- Impact the rest of our work
- Tell us what you don't like
- Tell us whether this is useful
- How we can make it more responsive

Roundtable 1

**Do the goals of NVT map to
the community needs and
requirements?**

Break

Click to add sub-title

***Information Sharing --
RAM and DPL-f***

Capt. Don Buckshaw

NVT Design

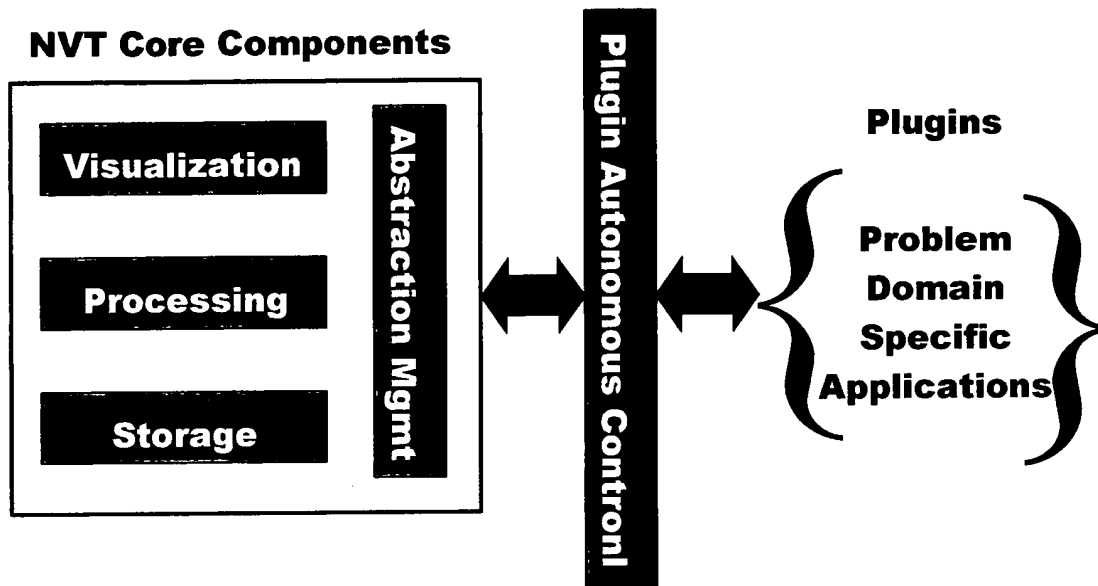
Architecture

NVT Architecture Goals



- Establish a framework that allows for the use of current and future risk assessment *plugins*
- Establish the foundation for a system that can resolve Ontological and Language issues
- Provide the user with a clear understanding of their present risk based on the most effective use of the current *plugin* set
- Provide the user with the capability to determine the most effective means to mitigate their risk

NVT Architecture Concept



- **Graphical User Interface (GUI)**
 - *Determine the GUI, do not invent new visualization techniques, but focus on applying work already done in other related areas, such as data fusion, message understanding, virtual reality, etc.*
 - *Understand that this probably at least a two part GUI, one for input and one for output*
- **Plugin Autonomous Control (fusion)**
 - *Focused on technologies to support automated integration of output from multiple risk assessment tools*
 - *Selected Fuzzy Expert System*
 - Fuzzy expert systems use a collection of fuzzy membership functions and rules, instead of Boolean logic, to reason about data

- **Visualization**
 - *HP OpenView*
 - *NetViz*
- **Processing**
 - *MS Visual C++ (Visual Studio)*
 - *Smalltalk (for use with ANSSR)*
- **Storage**
 - *MS Access database*
 - *Oracle*
- **Plugin Autonomous Control**
 - *FuzzyCLIPS - an extension of standard CLIPS that allows for the use of fuzzy facts and fuzzy rules which contain both membership functions and certainty factors*

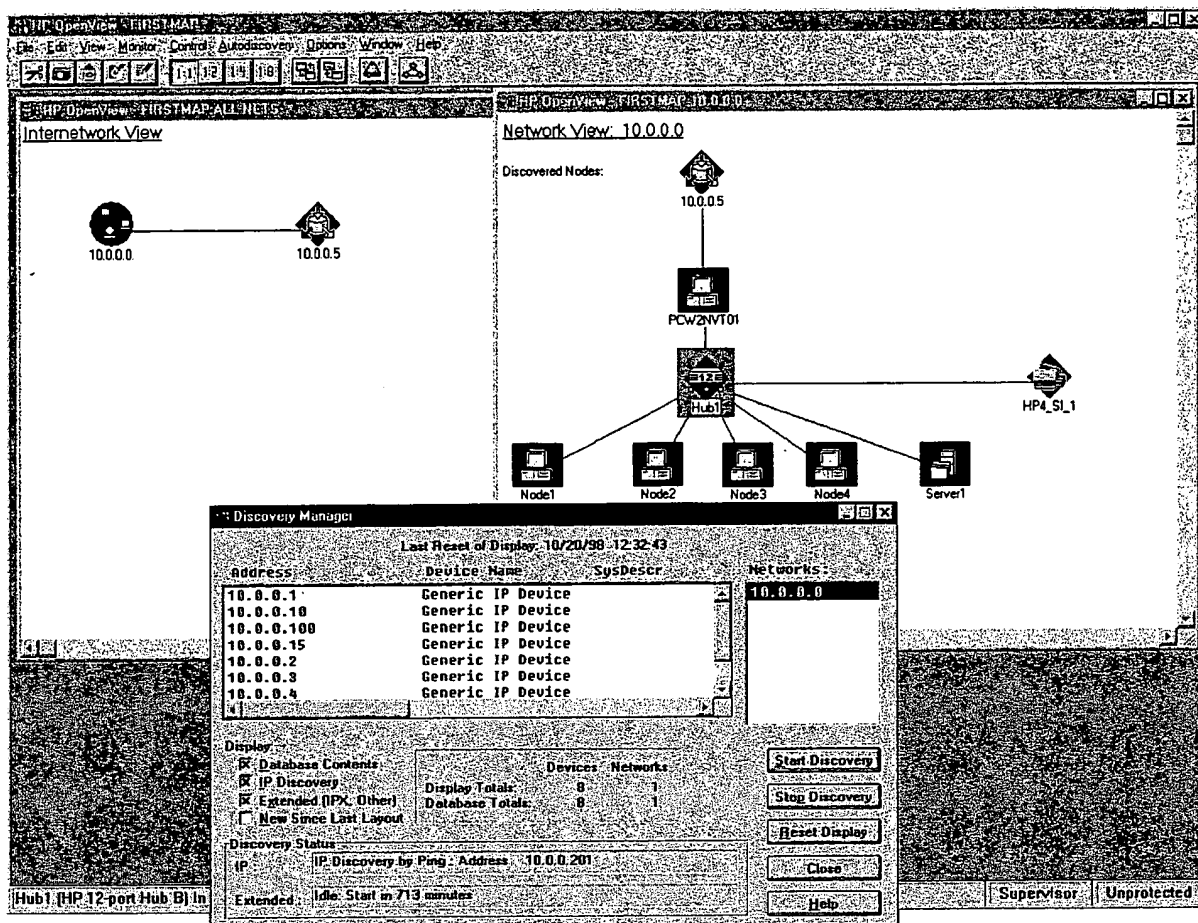
- **The integration of three distinct risk analysis/ vulnerability analysis reasoning engines into a proof-of-concept prototype**
- **One tool was chosen to represent each of the different categories of vulnerability tools**
 - *ANSSR was selected as a prime example of a legacy reasoning engine*
 - *ISS Internet Scanner was selected as an example of a “live” vulnerability tool*
 - *RAM was selected because of our experience using it for large scale, highly complex problems such as the power distribution system and because it was selected for the Secret and Below Initiative (SABI) Risk Analysis*

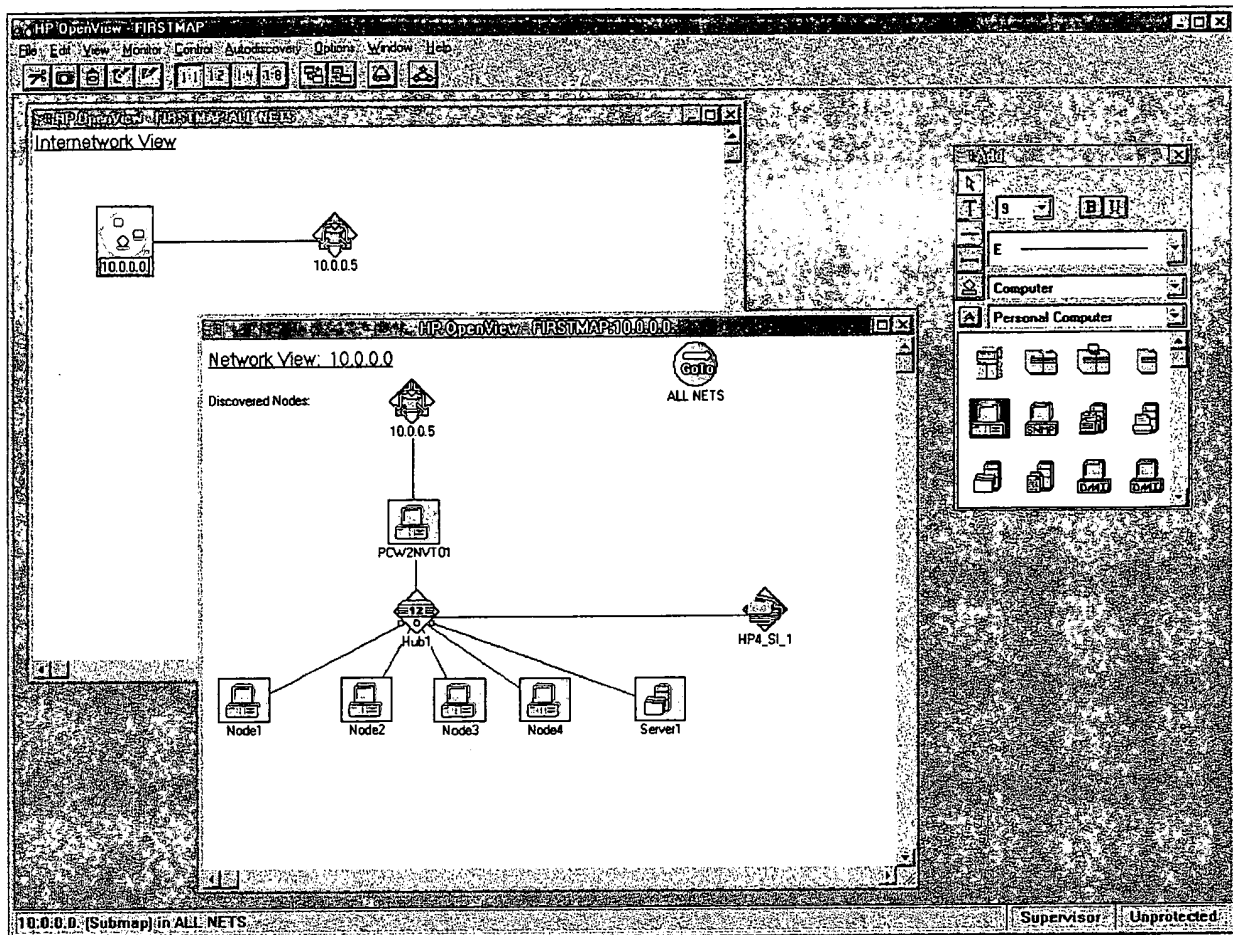
- **Automatic Discovery**

- *Given IP address of the default router, it searches for computers & other devices attached to the network*
- *Performs an active search, pinging possible IP addresses on the network*
 - Adds whatever response info it receives to its network map

- **Manual Network Diagram**

- *Provides a method to draw a proposed network*
- *Properties of each network node can be edited*
 - Add details to provide complete logical network planning
- *Can represent an entire network on a map by using a subnetwork icon*
 - Detailed map of the subnetwork can be linked to this icon and be displayed by double-clicking the subnetwork icon



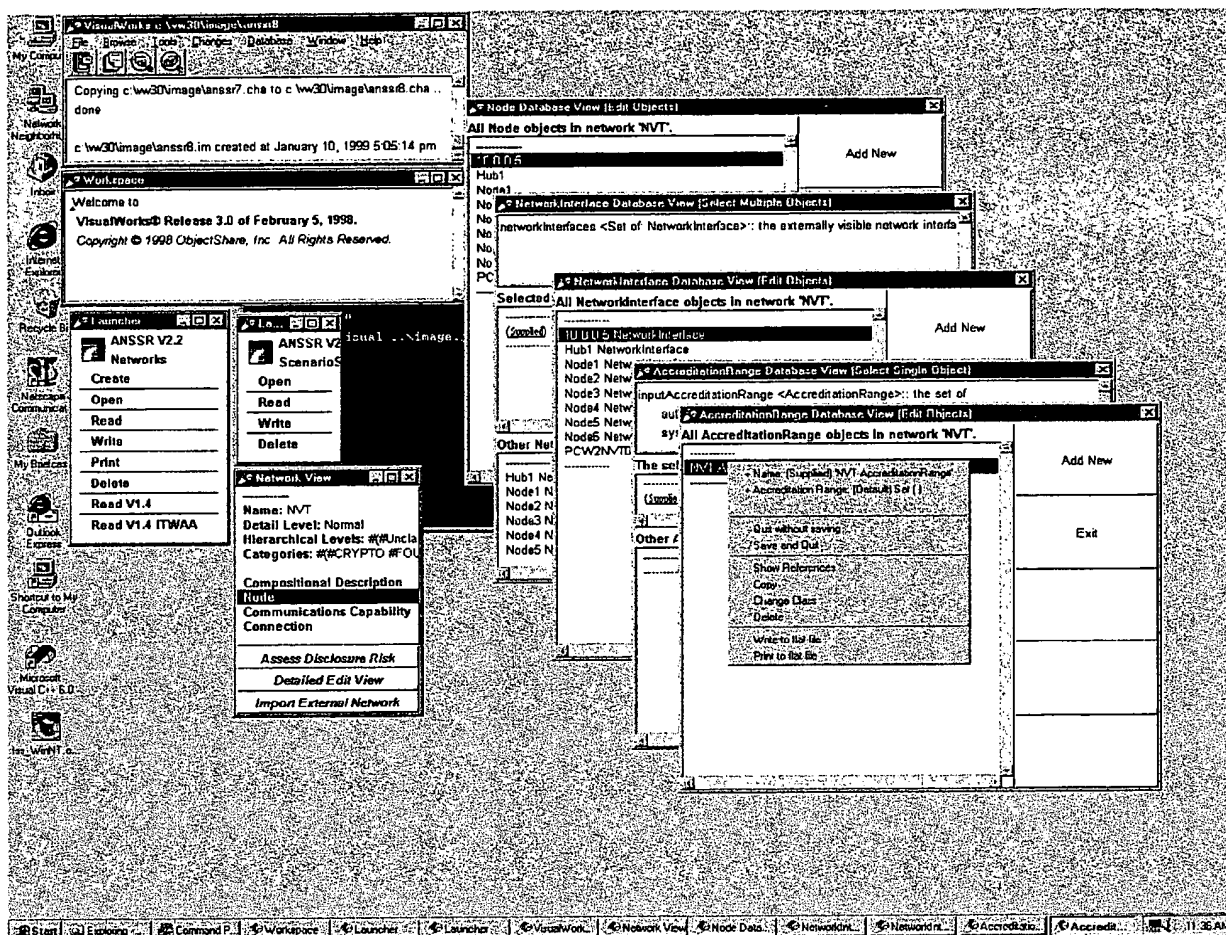


- **Data Assets**

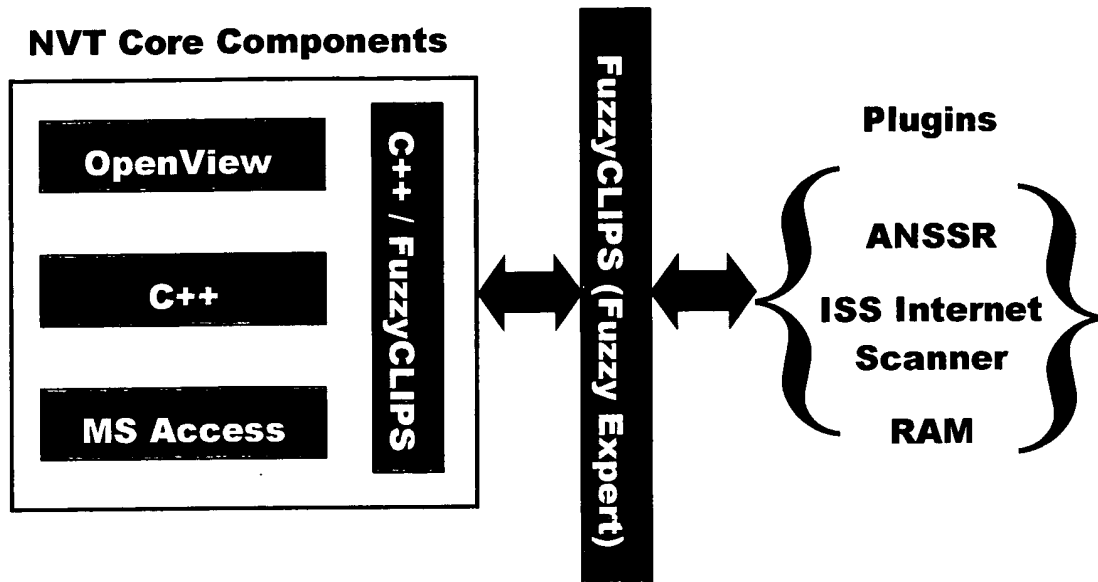
- *Primary object used in risk assessment*
- *Vulnerability of assets across network and through the user communities*
- *Represents protection mechanisms*

- **Use**

- *Requires Smalltalk*
- *Manual Entry through numerous menus*
- *Textual representation of Network*
 - *No visual representation*
- *Final risk assessment is a text file*

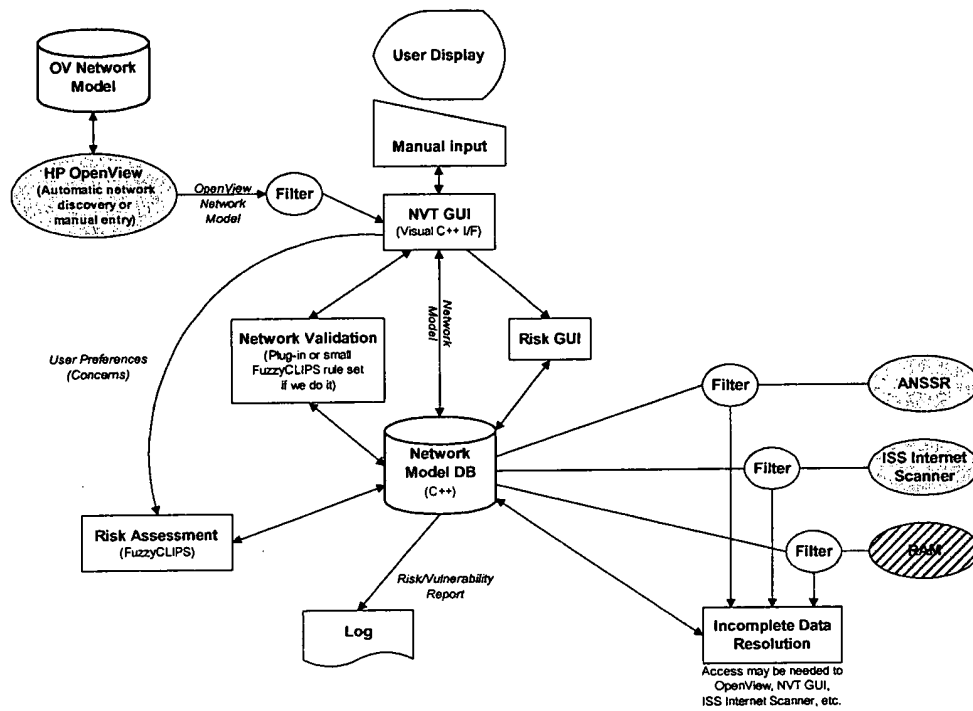


- **Scans existing network for vulnerabilities**
 - *Good assessment of system configuration errors*
 - *Information for system and network configuration may be used to setup ANSSR models*
 - *Input policy and session files control the scan*
- **Maintains scan results in Access database**
 - *Delivered with capability to export directly to Microsoft Access*
 - *Scan results easily imported to NVT through SQL*
- **Has discovery capabilities**
 - *Appears more reliable then OpenView*



NVT Prototype Architecture

HARRIS
Electronic Systems



Working Lunch

Click to add sub-title

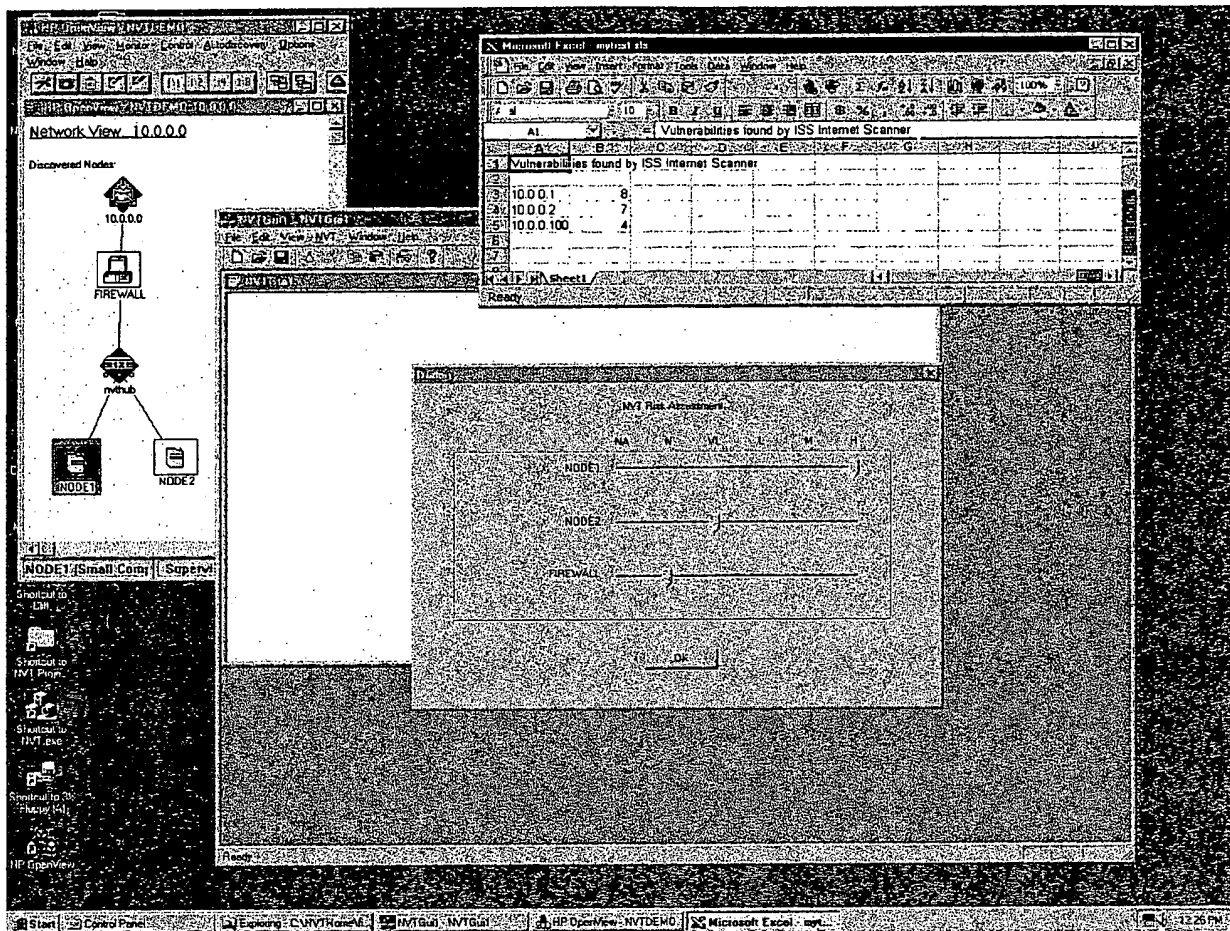
Demonstration

NVT Proof-of-Concept Prototype

Prototype Demonstration



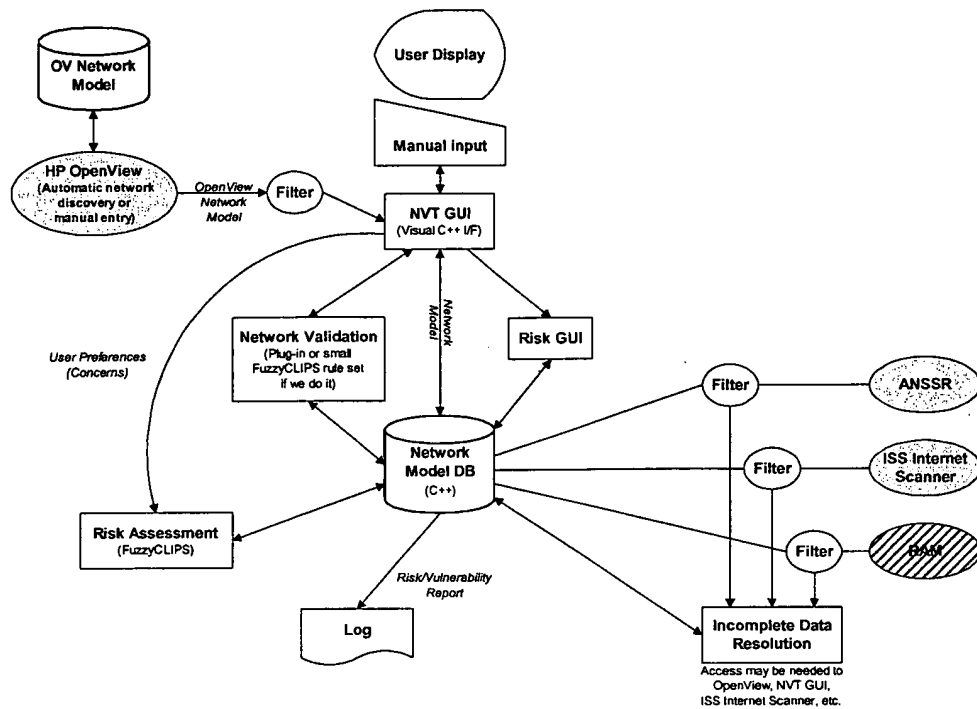
- Automatic Discovery
- Manual Network Diagram



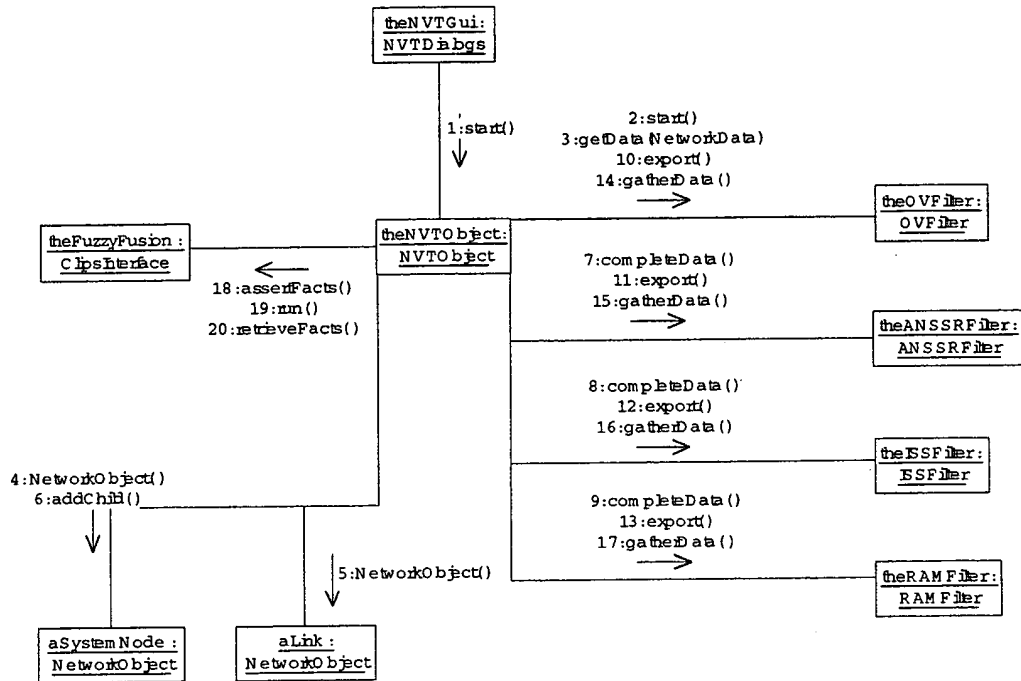
NVT Design

Object Classes

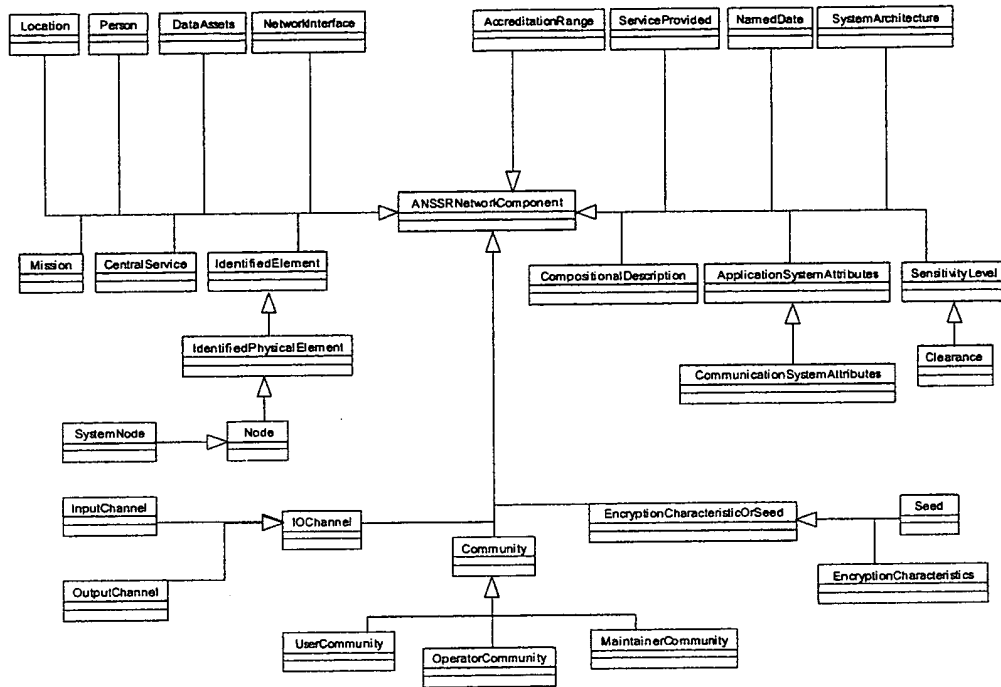
NVT Prototype Architecture



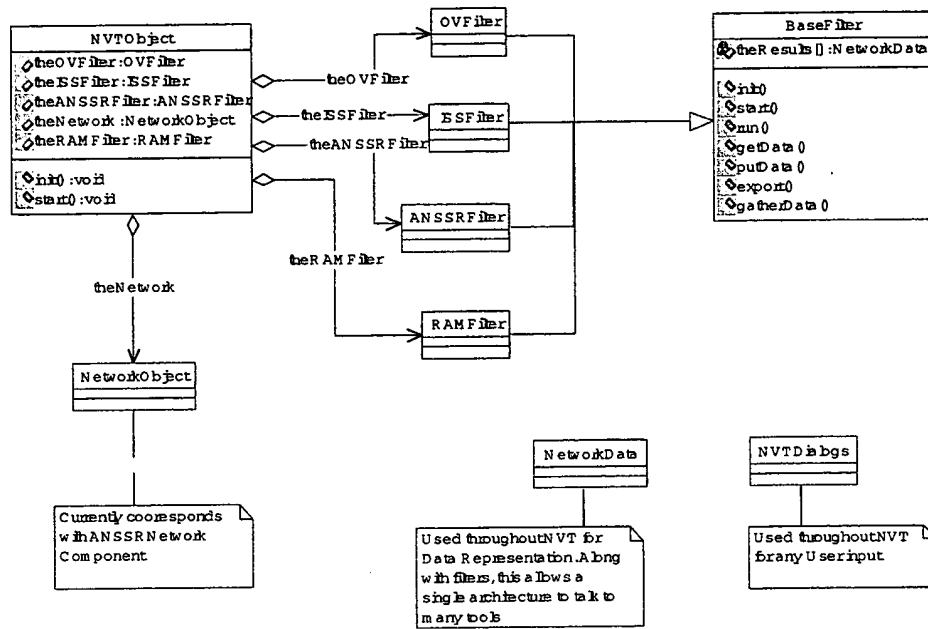
NVT Message Trace



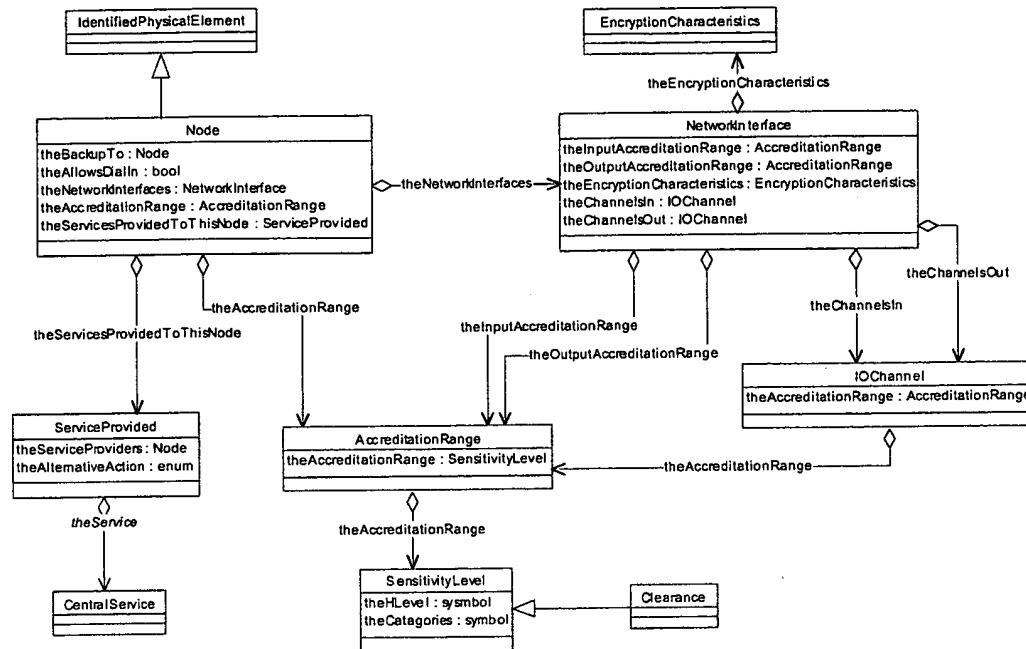
Required Classes for ANSSR

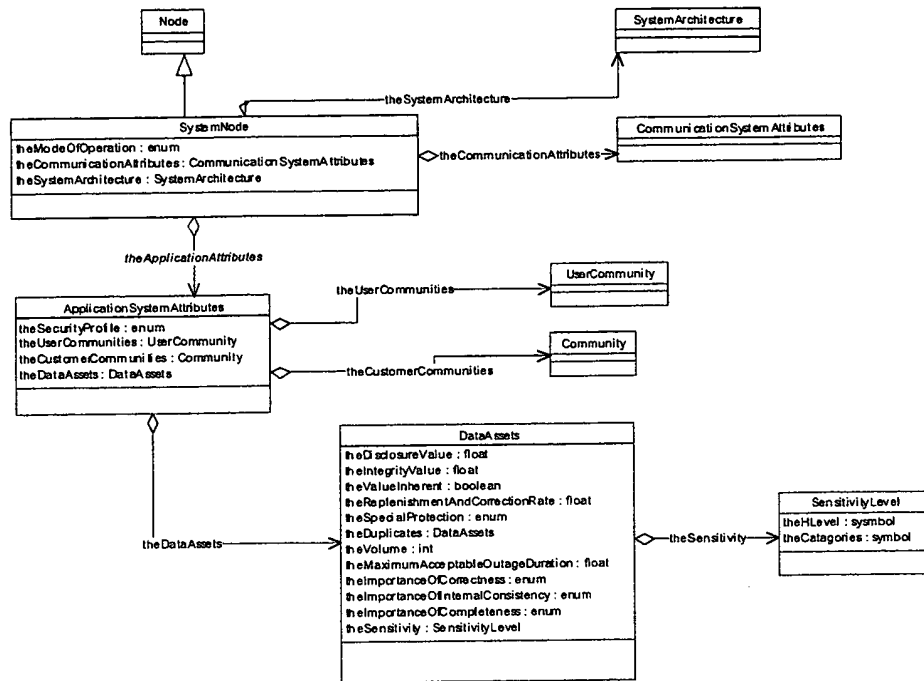


Class Interaction for ANSSR

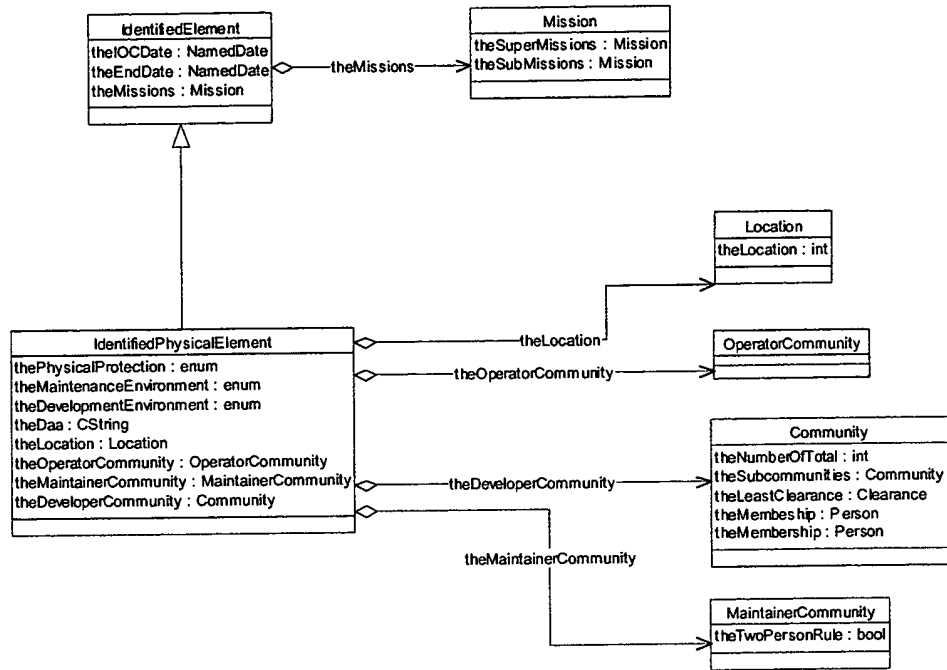


Node Representation

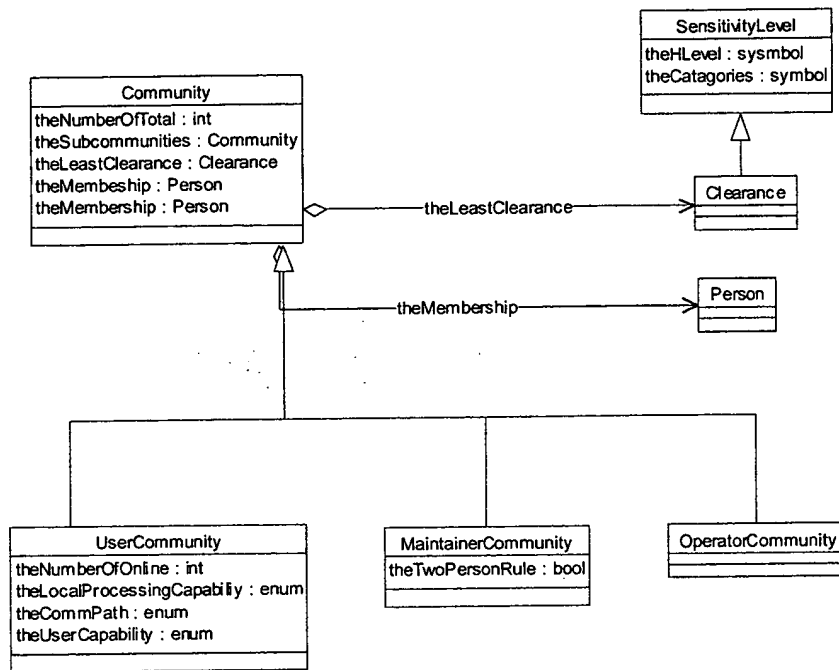




Identified Physical Elements



Community Representation



Break

Click to add sub-title

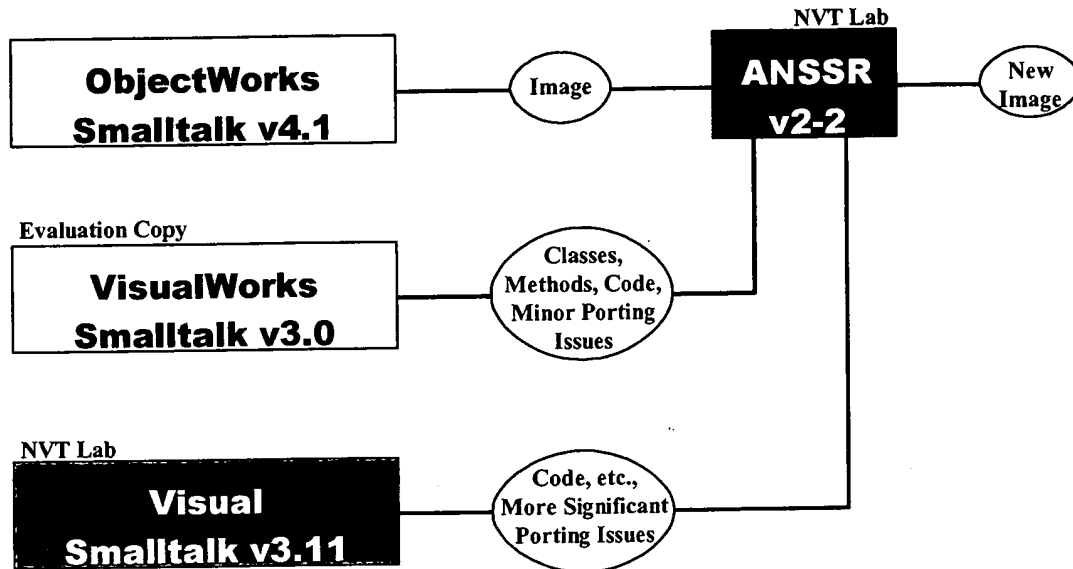
COTS Integration Lessons Learned

Click to add sub-title

- **Supplies extensive API, not always a good thing**
 - *C++ API several versions behind current MS compiler*
 - Limited 32-bit support
 - *OpenView designed for embedding and executing compliant applications from within OpenView itself*
 - *Communicating with OpenView from an external application not well supported*
- **Final communications required files**
 - *OpenView API not thread safe.*
 - *Full duplex communications through available IPC not possible with the OpenView API*
 - *Network received from OpenView through a file*
- **Auto discovery quirks in the NVT Lab environment**

- **Designed to run standalone, therefore no supplied API**
- **Required version of Smalltalk no longer available**
 - *Encountered challenges in integrating this tool under Visual Smalltalk due to Smalltalk compatibility issues*
 - *ANSSR 2.2 written in ObjectWorks Smalltalk version 4.1*
 - *Acquired alternate Smalltalk (Object Share VisualWorks 3.0, a readily available successor to ObjectWorks)*
 - Solved most compatibility issues
 - ANSSR has now been successfully built under VisualWorks 3.0
- **ANSSR delivered with code**
 - *ANSSR has now been further modified under VisualWorks to integrate with NVT*

ANSSR Integration Issues



ISS Internet Scanner



- Purchased, installed in NVT Lab, and tested on the test network
- No major problems associated with integration and use in NVT are anticipated at this time

- **Oracle originally selected**
 - *May need to eventually use for two reasons*
 - Scaling to larger networks (e.g. bases, multiple bases forming a command)
 - Object representation (Oracles Object-Relational extension)
- **Switched to MS Access**
 - *Ease of Use*
 - *Compatibility with ISS Internet Scanner*
 - *Excellent DAO support with Visual C++*

- **Harris/NSA working CRADA for use of RAM in NVT**
 - *Pending NSA legal review*
- **Current plan is to use the Excel spreadsheet version**
 - *Stable*
 - *Good experience base at NSA (R52/P5)*
 - *Eliminates procurement lead time*
 - Applied Decision Analysis (ADA) building it into DPL-f
 - Nobody at ADA has a price for the product
 - *RAM spreadsheet is recognizable*
 - *Used in SABI Risk Analysis Assessment*
- **However, may need to consider DPL-f**

- No major issues yet
- Seems to integrate well with Visual C++ based on testing performed to-date

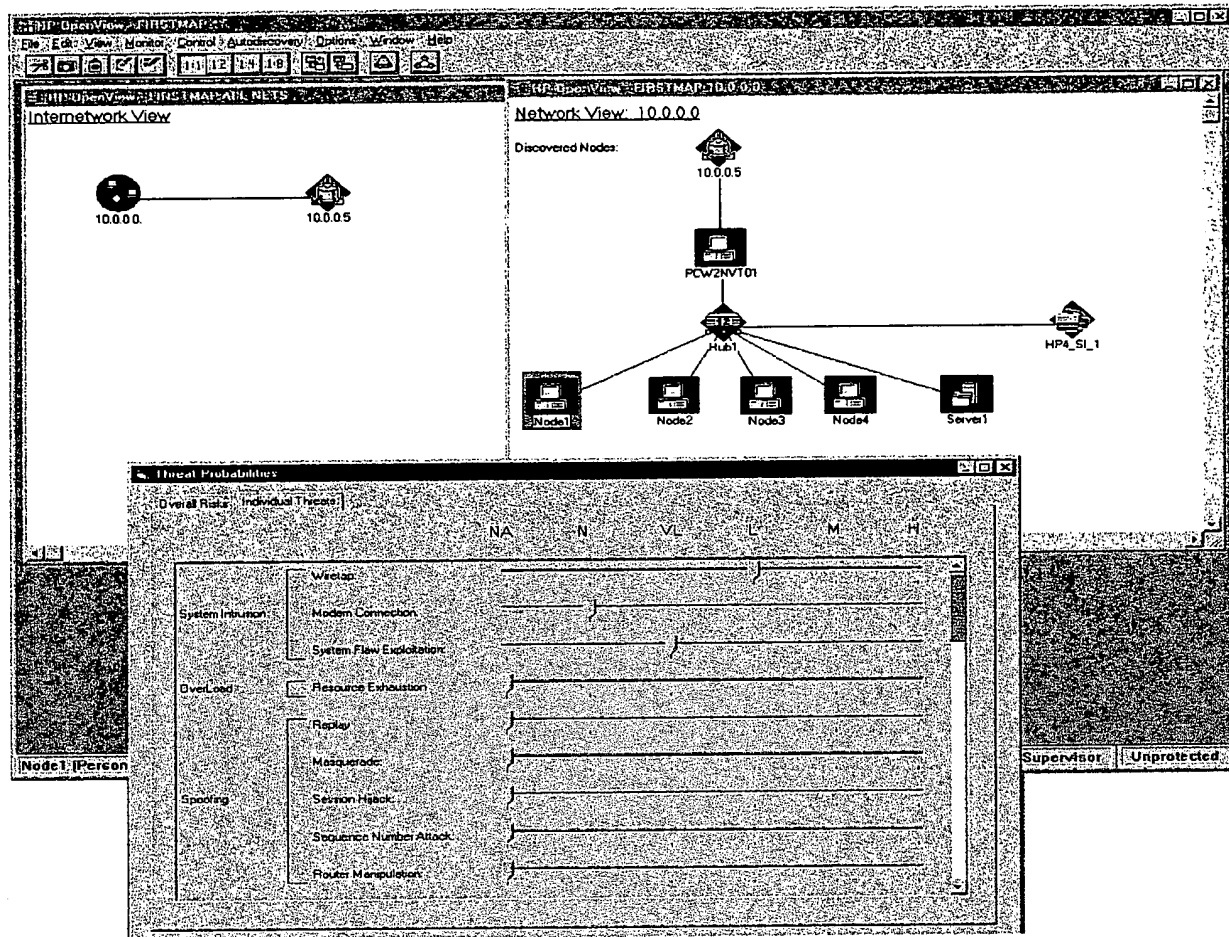
Plans for Next Quarter

Click to add sub-title

- **Complete the initial NVT Proof-of-Concept Prototype**
 - *Enhance the ANSSR I/F to catch more of what is there*
 - *Get CRADA with NSA completed to acquire RAM*
 - *Integrate RAM*
 - *Develop Fuzzy Expert to perform to fusion on outputs from our 3 risk assessment tools*
 - *Complete Graphical User Interface (GUI)*

- **Network Node Evaluation**

- *Show attack probabilities and vulnerabilities for any node on a network, even a subnetwork*
- *Provide methods for the user to describe the types of attacks and security risks that are of concern*
- *Allow user to fine-tune this information for various nodes on the network as well as establish a default value for the network*
 - This fine-tuning provides a greater level of detail for FuzzyCLIPS to provide a more accurate summary of the risk assessment



- **Integration and Test (in Melbourne)**
 - *The final integration/demonstration testing, that determines removal and/or documentation of the problems*
- **Ship Equipment to AFRL/RRS**
 - *Pack it all up, and send it out*
- **Deliver, Demonstrate and Test (in Rome)**
 - *Take it to Rome and make it happen for final sell-off*
- **Complete the documentation**
 - *Demonstration Plan*
 - *Software User's Manual*
 - *Final Scientific & Technical Report*

Future Plans

Beyond NVT

Future Enhancements

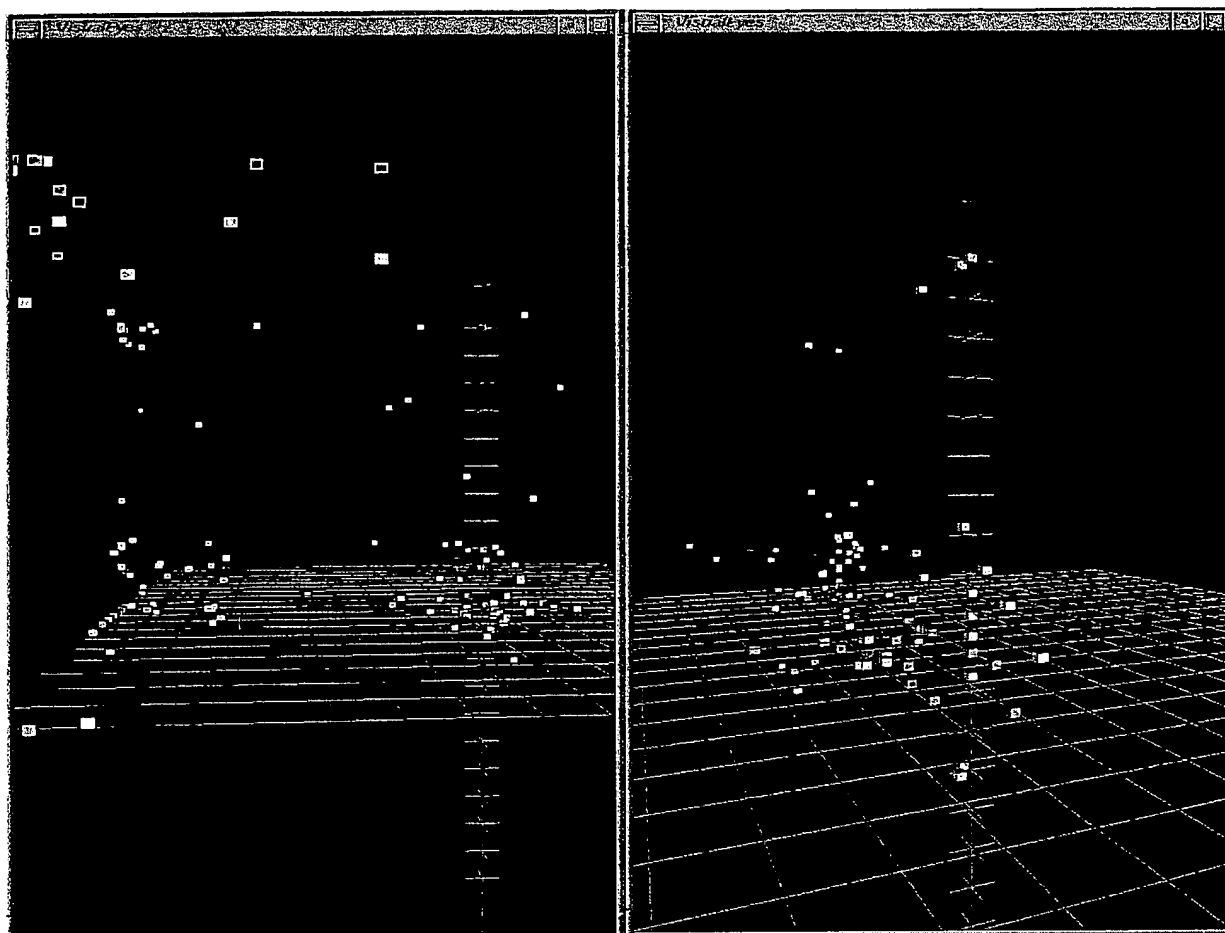


- **Replace HP OpenView as the Visualization tool**
 - *Single interface for entry of data for use by multiple reasoning engines*
- **Incorporate Static Vulnerability Database(s)**
 - *SEI's CERT and Harris STAT*
 - *More comprehensive vulnerability analysis of a system with respect to known vulnerabilities*

- **Vulnerability Thresholding**
 - *Minimizes continued computation when an aggregate vulnerability level exceeds a user defined limit*
 - *Allows user to define own vulnerability tolerance level, which supports tailorable definitions of acceptable levels of vulnerability.*
- **Knowledge Translation Ontology**
 - *Provides a common frame of reference for all tools & DBs*
 - *Facilitates deriving knowledge collected from other applications and existing tools, addressing problem of incomplete data for a given vulnerability assessment*

- **Temporal-based Reasoning and Vulnerability Modeling**
 - *Accounts for time required to exploit a known vulnerability as part of the system assessment process*
 - *Enable user to perform a vulnerability assessment that takes into account the time required to exercise a given vulnerability*
- **Vulnerability Trade-off Visualization**
 - *Use n-dimensional visualization technology*
 - *Allow user to perform what-if optimizations among performance, functionality, and countermeasures*

- **VisualEyes**
 - *SGI Platform*
 - *View 3-D and n-D data sets*
 - *Information Retrieval application*
 - *Open platform*
- **Risk/Vulnerability Trade-off Analysis**
 - *A system architecture is assigned values for security, functionality, performance, availability and survivability*
 - *Display similar to text retrieval*
 - *Cube represents a particular architecture design*
 - *Two 3D views displayed simultaneously*
 - *Security, functionality and performance*
 - *Security, availability and survivability*



Roundtable 2

Feedback on Initial NVT Demo

Wrap Up

Click to add sub-title

Action Items



- **Open Action Items**

- *HAI #11: Provide AFRL with the cost breakout per tool option for NVT and the NVT core elements*

HARDWARE	COST
NT Workstation	\$5130
SOFTWARE	
FuzzyCLIPS	Freeware
HP OpenView	\$950
MS Visual C++	\$495
MS Access DB	\$299
Visual Works 3.0 (SmallTalk)	\$2375
ANSSR	GFI
ISS Internet Scanner (30 user minimum license)	\$2975
RAM	GFI
TOTAL	\$12,224

Action Items



- **Open Action Items**

- *HAI #9: Provide AFRL with a Harris IP address to facilitate transfer of AFIWC Vulnerability/Threat data*
- *RAI #4: AFIWC to work through Dwayne Allain to provide access to their vulnerability/risk assessment tools*
- *RAI #5: Dwayne Allain to investigate providing the CTAPS Air Tasking Mission Planning video as illustration of the battle/attack planning process*

Action Items



- New Action Items ?